Privacy and Security Tiger Team
Draft Transcript
March 23, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good afternoon, everybody and welcome to the Privacy and Security Tiger Team. This is a FACA call, so there will be opportunity at the end of the call for the public to make comment, and a reminder to the workgroup members to please identify yourselves when speaking.

A quick roll call, Paul Egerman?

Paul Egerman – Software Entrepreneur
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Latanya Sweeney? Gayle Harrell? Josh Lemieux? Judy Faulkner?

Judy Faulkner – Epic Systems – Founder
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
David McCallie? Neil Calman? David Lansky? Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Micky Tripathi? Rachel Block? Christine Bechtel or Alice Brown?

Alice Brown – National Partnership for Women & Families – Director HITP
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
John Houston?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Wes Rishel?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Leslie Francis?

Leslie Francis – NCVHS – Co-Chair
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Adam Greene?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Lisa Tutterow?

Lisa Tutterow – Office of the National Coordinator – popHealth Principal
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Theresa Hancock from the VA is on. Did I leave anybody off?

Joy Pritts – ONC – Chief Privacy Officer
Joy.

Neil Calman – Institute for Family Health – President & Cofounder
Neil Calman.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you all. I'll turn it over to Deven and Paul.

Deven McGraw – Center for Democracy & Technology – Director
Thank you very much. Thanks to members of the tiger team for joining us on what is this afternoon for those of us on the east coast, and late morning for the west coasters. Welcome also to members of the public who join our calls. We appreciate you paying attention to what we're doing and providing us with input. It's very helpful.

I wanted to quickly go over what's on our agenda today, because it's a pretty full plate and we're going to try to do a little focusing in order to meet some deadlines that are associated with stage two of the financial incentive program. So we're going to begin by picking up a bit where we left off. You'll recall that at our last call, we started to talk about policies around patient access to information in an EHR. We're going to continue that but we're going to try to focus a little bit today on policy issues that are relevant to triggering the need for certification criteria for EHRs in stage two, as opposed to policy issues that don't necessarily have a technical component but that nevertheless need to be addressed. And the reason for that is that we know from experience in teeing up some meaningful use recommendations on privacy and security in round one that CMS was not terribly enthusiastic about us including additional policy requirements beyond HIPAA, and they actually said this in the final meaningful use rules, in the meaningful use criteria. But they were open in stage one, and remain open from what we understand, to making sure that the technical component that supports certain privacy policies that are associated with meaningful use objectives are included. So that they can be part of certification for stage two if they involve functionalities that aren't necessarily present in EHRs today, or may not be because it wasn't clear in stage one.

Just to give you an example of what we mean by that, there is right now a recommendation for patient portals for the patient access provisions of meaningful use. Of course, in order to support that there is a need to properly identify and authenticate and track patient access, which has policy components to it, of course, but also would need to be supported by technical functionalities in an EHR. Because we have been asked to try to tee up those policy recommendations that have that technical link and a subsequent need for additional criteria to be added in certification of EHRs for stage two, we've been asked to try to focus on those policy issues first so that we can tee those up for the April Policy Committee meeting.

So our discussion on patient access is going to be focused on authentication in particular, we'll talk a bit about authentication and whether or not there's a technical component to that piece of it, but again we're not saying that we won't address the other policy issues that are raised by patient access to information in a provider EHR. But we're trying to meet some deadlines for teeing up our policies that have related certification criteria, because there's additional work that needs to be done by the Standards Committee, and so that ball all has to get rolling.

We'll do patient access. We're going to start with a brief presentation by someone from the VA on the My HealtheVet portal with the download function, otherwise known as the Blue Button Initiative. Paul will be the leader of that discussion. We will then turn to looking at what are the existing Meaningful Use Workgroup recommendations and some of our tiger team recommendations on privacy policy that are linked to technical functionalities that would need to be included in certified EHRs and try to tee up that discussion as best we can on this call today. We might have to continue to do some work on it off line in order to get this done by the April Policy Committee meeting, but it's a little bit of a gearshift there. But it should all be familiar territory for us because it is covering issues that we have talked about before.

Then we do have some wordsmithing slides on the user authentication discussion that we've spent about the last month talking about. We just want to spend a little time at the end of the call taking a look at that language, but trying not to wordsmith it on the call and asking for your assistance off line to try to finalize that, particularly those aspects of it, again, that have technical components that will need some work by the Standards Committee.

I'm going to stop and make sure that I've articulated that in a way that makes sense and is clear. Paul, was there anything that you wanted to add?

Paul Egerman – Software Entrepreneur
Great job, Deven. I do not have anything to add.

Deven McGraw – Center for Democracy & Technology – Director
Okay. Does anyone have any questions before we jump in? I think you'll see the flow of this in the slides a little bit better once we get started. But I want to lay the framework for how we're going to try to focus the discussion today. All right, terrific. Paul, let's get started with patient access.

Paul Egerman – Software Entrepreneur
Hello, good afternoon and good morning. We want to talk about patient access, which is limited to the concept of identity proofing and authentication, and also in terms of terminology, the reason why we're doing this relates to what's going to be, we suspect, in stage two of meaningful use, we don't know for sure, is this concept called the "patient portal." The patient portal, some people might call it a tethered PHR, is another terminology, but it's sort of like an access port on the provider's EHR system that lets patients view their medical data.

Judy Faulkner – Epic Systems – Founder
Paul, one thing is that sometimes it's called a shared PHR, shared instead of tethered, which is actually a better word.

Paul Egerman – Software Entrepreneur
Okay. Thank you, Judy. There is an aspect of the terminology that definitely needs to be straightened out or clarified. But this concept of patient portal, or as Judy just called it, shared PHR or tethered PHR, apparently it's got 600 names to it, but basically it allows a patient, or perhaps the patient's proxy, to look at their medical data, that's generally what is allowed to happen. Sometimes there are other things they can do, like sometimes you can do administrative transactions relating to appointments or bill paying or perhaps send a message to a provider, but it's basically access to the information. The way we wanted to start the discussion, we are limiting ourselves to the issue though of the patient identity proofing and

authentication. The way we wanted to start was we have here to present, talk to us, is Theresa Hancock, let's see if I can get your title correct, Theresa, you are the Director of Veterans and Consumer Health Information Office. I'm not sure I got that right.

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
Informatics Office.

Paul Egerman – Software Entrepreneur
Health Informatics Office. Thank you. She originally submitted a slide deck to us that gave an overview of what the VA does, which I looked at the slide deck and I thought it was spectacular, and I actually feel terrible that we're not showing that whole slide deck. But I'm only asking her to talk about just the issue of how to handle identity proofing and authentication for patients. It feels a little like going to Disney World and the only thing you're interested in is what is the turnstile that lets you get into the park, whereas, you're not interested in the whole rest of the process. Hopefully we'll get you back, though, Theresa, to talk about the rest of what you're doing. Whatever insights you have to share on how you're handling the identity proofing and authentication at the VA would be very helpful.

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
Great. Thank you so much for inviting me as a guest. I appreciate it. I actually liked your analogy, and I'll probably steal it, with Disney World. The two basic questions I want to answer today is how does the VA handle patient identification, authentication, audit trail and specifically through Blue Button download capability. It actually is no different than what we do today. Whether it's the Blue Button download capability or not we use a process called In Person Authentication, which allows the veteran to have an upgraded My HealtheVet account. An upgraded account means that they can have access to ... or computerized patient record system or Vista, which is the VA's hospital record. We're soon going to rename this to In Person Proofing or IPP instead of IPA. It uses security measure as a process to verify the My HealtheVet user's identity. As a prerequisite, we ask that they initiate a My HealtheVet account and when they go into the account, they must indicate that they are a VA patient. That's the trigger when they register that will allow them to get the upgraded account.

They must also view one of four videos and they can also do that online or at the facility. They need to read and sign a VA release form. They can do that online or in person. When we worked with general counsel, you and I as a patient go in and we need to sign a form each and every time we visit the facility and specify what type of information we want. Our general counsel actually said for veterans we'll let them have the capability to fill that form out once in a lifetime. So they need to fill it out online or in person and submit it to the designated person. Veterans actually said that they thought after a while that that was too much, and I'll talk about a little bit about some alternatives we have given them. While they're there they must also present two forms of government issued ID to a qualified staff member, and the person who's designated, who's qualified is our Health Information Management team or Medical Records department.

After they complete those steps in person, then the designated staff actually has a module called an administrative module that they go in to a check box and they check each of those steps off. When they complete the last step it actually sends a message through our Master Patient Index system, and that locks the account down so that the key information that was validated for identity authentication purposes can't be changed. Once they do that, a flag gets sent to our computerized patient record system, in CPRS, where it's viewable by the providers who have access to the patient record. That flag serves two purposes. It's used to enhance communication for providers, and it was our number one request from our providers on how can I tell if my patients now have access to online information.

So if they're in medical records, they see that enhanced flag, two communication points. One, if it's an abnormal result, they can look at the flag and say, my patient can now access this information online and they don't need to physically come here. Perhaps I need to ... chat notifying them that they have an abnormal result. Two, it serves as a communication mechanism. Perhaps they will write different or perhaps not. We know from history, looking at old notes and records, that sometimes the information wasn't written particularly for a patient, and so it may prompt them to write a little bit different.

That initially was the steps and approach that we took for the in person authentication identification. When the veteran says that's too much, once in a lifetime, especially those in rural areas, we went back to the general counsel and they approved that power of attorney, legal guardian or designated home nurse, designated by ... would be allowed in the veterans home to do the same process, to request all the information. When they got back to the facility, they would turn it over and then the designated person could put it in the ... system and it would be accepted.

We also looked at alternatives. What we're doing now is working on DS log-ins with the Department of Defense so that we grandfathered those who have a DS log-in Level 2 credential and they have a My HealtheVet upgraded account that underneath we will connect the two accounts so they don't need to reapply if they already have a DS log-in too. So that's something that's in the works now with the Department of Defense and the eBenefits group in the VA. We're also working on, with our identity management group, online authentication. Again, looking at those that live in the rural areas who just do not meet that criteria that we had set previously. The other alternative we have ... today is using eAuthentication in the federal group, to be able to come in and use a single identification credential as a sign-on process for My HealtheVet when you are a member.

Then looking at it from an audit trail perspective and the Blue Button, we created a user screen that enables them to track the monitor access to their account and it lists things like their user name, what areas that were accessed, what time, and it's dated so that the user can track themselves and their actions. But more important when we get to delegation or surrogacy they will be able to track their accounts and the users that come in, whether it's a family, advocate, provider, they will have that capability on their own. In addition, the system itself keeps track and has its own system log files that tracks the identification of those coming into the patient's account.

When we looked at policies for the Blue Button, we did work with our … privacy and security subject matter experts. We don't actually call them policies. The … group has what we call directives and we've included information specifically for downloading the audit trail, and we use HHS' meaningful use policy document as a guide, and so we incorporated I believe all of the information that was recommended by HHS into our directive. So we're using it for the audit trail, we're using it for the education piece, we're using it, right now we have a seven day delay, information coming from the EHR to the PHR, to give the physicians time to review. The DoD uses four days meaningful use, recommended four days, so we have a configurable field so we're going to change it to four days ... DoD following it and DoD is our partner in everything that we do. We've actually worked with CMS as well on specifically the Blue Button download. We have several other federal agencies that have expressed interest in working specifically with the Blue Button. So we have a dedicated policy workgroup as ... privacy and security and others' general counsel, and we're using meaningful use .... Any questions?

Paul Egerman – Software Entrepreneur
Yes. Theresa, great presentation and thank you very much. One thing that was not clear as you were speaking, you were talking about how you do the identity proofing and how you're doing the audit trails, but when patients actually sign on to the system is it like one factor, so user name and password?

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
Yes, that's correct. They fill out a registration screen and they get a user name and password, that's a registered user. They have access to general health content, authoritative content. They have access to self-entered logs where they can track and monitor information on their own, some assessments and worksheets. If they get an upgraded account then that allows them to have access to the EHR ....

Paul Egerman – Software Entrepreneur
But it's basically what I think might be called one factor authentication, so user name and password.

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
That's correct. Well, two factor in the—

Paul Egerman – Software Entrepreneur
I'm sorry. Did somebody have a question?

M
This is—

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
Well, it's going in face-to-face and user name and password.

Paul Egerman – Software Entrepreneur
Yes, face-to-face in terms of identity proofing.

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
That's correct.

Paul Egerman – Software Entrepreneur
Then once that occurs you give somebody a user name and password and they can access their system with user name and password.

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
That's correct. We're going to online authentication for OMB to have at a level three.

Paul Egerman – Software Entrepreneur
Great. Wes, it seems like you had a question.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well, you actually answered the question with your question. I just wonder if Theresa could elaborate on what she means by going to online authentication for, I assume she means threat level three or assurance level three?

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
Yes, that's correct, so that the patient can do it from the convenience of wherever Internet access is available. Right now, our identity management is looking at several products where it would be question based and it's something that the veteran knows.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
We're trying to distinguish between the things you do one time in order to be sure you are talking to the right person, which we're calling identity proofing, and the things you do frequently, every time they want to access the system, which we're calling authentication. Some people do use this notion of questions the person will know as a way of identity proofing. Other people, like banks, use it as a backup mechanism for authentication, and I wasn't quite sure whether you were planning to use these questions the veteran would know for authentication or for identity proofing.

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
For identification. Also, what I left out is that we're looking at mobile devices and we're currently working on that so that that's something that they have.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So then they might be able to log in somewhere by having a special code be texted to their phone and then they would type that in. Is that what you're referring to?

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
Yes, that's correct. We found that currently right now we have over a million users and of those million users 95% have given us their e-mail addresses and a significant portion of them have also indicated in some of our surveys that they have cell phones.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So that would be another way then, a stronger means of authenticating veterans when they want to connect to the system. Would that then replace passwords, or would it be for the higher level of access, or just if the veteran wants stronger protection?

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
It won't replace it. It will be another modality by which they can get stronger access.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So if the veteran's concerned that nobody else will be able to see her data, she could ask for this special level of detection, is that right?

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
That's correct.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Okay, thanks.

Paul Egerman – Software Entrepreneur
Great. Any other questions or comments?

Deven McGraw – Center for Democracy & Technology – Director
Yes, just one. Theresa, it sounds like you might actually be doing a little bit of balancing. You can correct me if I'm wrong about this, between when you've got in person identity proofing, that feels like such a strong identity proofing to the VA that authentication can require just one factor of a user name and password. Whereas, if you're allowing people to be able to establish accounts without the face-to-face you might be doing some additional work on the authentication side to provide some additional security. Is that a correct way to surmise what's going on here? Or, am I mixing apples and oranges?

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
No, that's correct, because we can't assume that everybody has a cell phone. So we need to offer different methods by which they can get upgraded and authenticated.

Leslie Francis – NCVHS – Co-Chair
I'm still not clear on whether you're talking about authentication of the individual accessing the system after the upgraded account has been set up, or the original identity proofing to make sure the person setting up the user name and password, getting that special number, whatever, is really the person they claim to be.

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
It would be the initial. They need to go into the facility. If they chose not to do that, they could actually, through questions answer only specifically things that they would know for identification purposes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That would be the one time while they were upgrading their account that they'd have to do that then.

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
That's correct.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
And then after that it would always be just user ID and password.

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
Correct.

Deven McGraw – Center for Democracy & Technology – Director

That makes sense, great.

Paul Egerman – Software Entrepreneur
Any other questions? Theresa, excellent job, thank you so much. I really appreciate your help and we also, again, appreciate the rain check on the rest of what you're doing, because it sounds like—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Paul, did the deck that we received, is that the longer deck that you were describing, or is there still another deck that we—

Paul Egerman – Software Entrepreneur
That's the deck I'm describing, but I wouldn't be surprised if they have other ones also.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Okay, thanks.

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
We do, and actually ... get a copy of that deck to send it to this workgroup and if they feel appropriate, they can distribute it. It talks about the things I just mentioned.

Paul Egerman – Software Entrepreneur
That would be great, because as you can tell, we're very interested in this entire area. Thanks, again, Theresa then, and again I'd love to spend more time with you, but unfortunately, we have this thing called a deadline that we need to try to address these issues. So for the—

Theresa Hancock – Veterans and Consumer Health Informatics Office – Director
Thank you.

Paul Egerman – Software Entrepreneur
I'm sorry, was somebody about to say something? Okay, so for these issues, again, we have these two different concepts and so I have a short presentation here that the good people at MITRE put together. So what you see on your screen is an outline of questions. Again, as Wes very clearly articulated, we're breaking this concept into two concepts: there's identity proofing and there's authentication. Identity proofing is verifying the patient's identity and under that there's four questions. Who performs the identity proofing? What method is used? What is acceptable documentation? Should the documentation be verified? The authentication process, again, remember is once the patient has whatever token or credential that they have, what is their process of proving that they are who they say they are. So that could be user name and password or it could be multiple other things.

That's the outline of questions. I'm going to rapidly walk you through, first, the identity proofing questions. So, again, the good people at MITRE put this together for us. The question is: Who should perform, who's responsible for actually doing the identity proofing? The suggestions that they put forward are, one is the patient's provider, and then they said an entity offering access. I think what they're referring to in the first one is the patient's individual physician, and the second one is the provider entity could be doing that, like Kaiser or Cleveland Clinic or UPMC. It also suggests another alternative is possibly a trusted third party, a notary public, maybe there's somebody who issues credentials, possibly a partner organization, perhaps the physician is part of an accountable care organization or some community activity, directed activity, and maybe that partner issues the credentials ... employer, somebody that can work in some models. So this is a number of answers to that question of who should perform the identity proofing. As I go through this I also am aware that there are people like Dixie who are on the phone who know this stuff like 100 times better than me. So feel free to jump in when I describe something that's not quite correct.

The second question is: What is the method that should be used to identity proof a patient? Typically, exactly as Theresa said, there's usually some form of documentation to prove the identity of the individual, and it's either in person or perhaps done remotely. The second bullet says here is in general in person identity proofing has traditionally been seen as arguably the most secure, so it's not a surprise that the VA started with in person identity proofing in terms of looking at all of that issues. Also, as Theresa said, there's an issue of sometimes how practical that might be, and so there's other alternatives in terms of the methodology. You can use information that's based on an existing and durable relationship. You can boot strap on other encounters. In terms of the existing relationship, you can use information about name, address, date of birth, last prescription obtained. I almost took a guess when Theresa was talking about their methodology they're looking at for online identity proofing that they would probably ask the individual some questions, and so that might be the kind of question you would ask the person and presumably they would know what was the last prescription, for example. That's the method.

The documentation that's used is picture IDs, frequently government issued picture IDs, financial account information. My son, who's in Indianapolis, told me recently at some event where he had to go to a healthcare organization they wanted him to bring with him a bill to prove his address. It was very interesting. Postal service address can be used. Certainly a long-standing relationship, if the parties know each other. There may be other things at the discretion of the proving entity and then the question becomes should the documentation be verified? And as it says here, there are two choices for that one, which are yes and no. Maybe there's more than two, I assume, but it seems like if one were putting together at least a straw man that would be the correct choices, in my opinion.

Next, I'm going to walk us through the authentication process. But the question is: As we look at this, what do we as the tiger team want to do with this entire issue? Do we want to say, well, these are the topics and each healthcare entity's got to make their own decisions knowing what they know about their populations? Do we want to say anything more about identity proofing policies?

Deven McGraw – Center for Democracy & Technology – Director

I found it very interesting that in Theresa's presentation from the VA where they started with in person identity proofing. They had a process where they got feedback from the veterans they served that led them to adopt other mechanisms in order to enhance the likelihood that people would sign up for this and be able to use it without having to go to the trouble of showing up in person where doing so would be burdensome. So I guess to me that points out a couple of things. One is the need for entities to establish their policy in a way that makes them comfortable, because they bear the risk if information is improperly accessed, but at the same time not setting the bar so high that no one is able to sign up for the portal. Secondly, rather than setting specific policy if there are any principles that we want to set here, given that, again, under the HIPAA security rule entities already have general obligations to protect data and make sure that only those people who are authorized to access it can access it .

Leslie Francis – NCVHS – Co-Chair

Deven, one of the most frightening things we heard at NCVHS at the Privacy Committee when we were doing a sensitive information letter was testimony from the folks who deal with abuse and domestic violence about how information in a medical record could be used. Not just for medical identity theft but for questions like stalking, finding out where somebody is now living if they get medical treatment. So anything that permits remote proofing but deals with information that, for example, an estranged spouse might know, and that would include Social Security number, is to me very scary. I think identity-proofing needs to at least think about information that the person would know but others who might not have their best interest at heart wouldn't know, and probably that needs to be information that's very close in time to the individual.

Paul Egerman – Software Entrepreneur

Leslie, great comment. I'm trying to understand, in terms of establishing policy or principles, maybe the principle that you're suggesting is that the methods that are used to do identity proofing should vary depending upon the sensitivity of the data.

Leslie Francis – NCVHS – Co-Chair

Well, but actually what I was suggesting was that to the extent that information in the medical record would allow you to locate the person, which isn't the kind of stuff people are going to think about as particularly sensitive, there's a risk. So I was suggesting that you think beyond just the medical information in the medical record, but the kind of information that might be there for purposes of identity theft, stalking, and the like. I agree with Deven that a basic principle is risk balancing and the convenience, but if you're going to go with the convenience of something that isn't in person, I think the principle has to be that it's something that we're really, really sure that only the individual and not close family members, estranged spouses, and the like would know.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Leslie, I want to be sure first that I understand, are you now talking about the information that would be used for identity proofing, or are you talking about the information that might be available to a person whose identity has been proved?

Leslie Francis – NCVHS – Co-Chair
I was talking about that I think the policies governing remote identity proofing need to have a pretty high floor because of the risks I was just mentioning.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I see. Then of course if this is a strong balancing act, I think one of the things we were reminded of by Theresa is that there are important patients in the healthcare system that are located rurally for whom travel is a burden. We are, to some extent, having to think of that constituency and the constituency of people who are in physical danger if some of their medical information gets out, and in fact, some of those cases overlap, it's not that you're going to say those are two different cases. So the question is, if we were to say, for example, all identity proofing for all remote access to a patient portal required that in person validation, then we would limit it to the cases effectively where we were providing services directly to the patient, either a person we could trust was going out to visit them for some reason, or we had them in the office and we could do the identity proofing in the office.

Leslie Francis – NCVHS – Co-Chair
There's another way to do it remotely, for example. You could have a telephone call that's directly with the patient. There's a lot of remote monitoring over the telephone. I'm not suggesting what the method should be and I'm not objecting to remote monitoring per se, but I am suggesting that a lot of the kinds of information, date of birth, Social Security number, financial information, that people might think of as, or maybe an individual knows it, are I think too risky. So I think the principle should be that when there is remote identity proofing it should be in some way unique to the individual.

Deven McGraw – Center for Democracy & Technology – Director
Right, and using methodologies and processes that are likely to be reliable in uniquely identifying that individual, I get that. A question came up in a domestic violence situation, but if you think about the incidence of medical identity theft and the way that consumer data, like a Social Security number and your address and maybe even a bank account number, is not that difficulty necessarily to get. You wouldn't necessarily want to have that basic information be the set of questions that would allow you to set up a remote account to an EHR.

Neil Calman – Institute for Family Health – President & Cofounder
I think the one exception to this would be that we need a mechanism for people to be able to establish an account, not to access information that's already in an EHR, but to establish an EHR remote access de novo without being present in the center. Because that whole process of being able to register yourself, put in an initial patient history and whatever, and then have an ability to confirm their identity when they actually have their first face-to-face contact, I just think it's important that we just make sure that we leave an opening for that to take place.

Leslie Francis – NCVHS – Co-Chair
Yes, that's what we were talking about.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think I heard Neil carving out a particular special case where it may actually be fairly easy to register himself as a provisional user and all you can do as a provisional user is put information in about yourself,

you can't see any information that you didn't put in yourself. Then when you're actually seen at the clinic you can upgrade from provisional user to user by one of our accepted ... of identifying proofing. I think that there's an awful lot of cases, someone who's just beginning in terms of a pregnancy and other cases where it should be tremendously valuable to have people be putting in their data before their first visit.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I would like to go back to what Deven said. She brought up the area of risks, and I think that we really should think about this in terms of risk and who bears risk, which in my opinion it's ultimately the provider organization if they give an account to somebody and it's the wrong person. I also would bring up the point that the HIPAA privacy and security rules don't specify for an organization the process they should use to decide whether somebody gets an account or not. I think the point that I think Deven was making, that maybe it might be more appropriate for us to recommend principles rather than strict policies.

I would also add that I think Theresa's presentation brought out a really good point, that not everybody is living in the same environment. In a rural environment, for example, a provider might want to use the local public health organization to help them identity proof. I think the policy we should leave up to the individual provider entity but should recommend some principles for that entity to use.

Josh Lemieux – Markle Foundation – Director Personal Health Technology
This is Josh Lemieux standing in for Carol Diamond. I'd really like to second that. We had a Markle working group look into this issue of providing individuals secure access in the context of their health information and we actually couldn't find any real objective measure or proof or documentation that in person proofing is actually more accurate than remote. The reality is it's very contextual, based on the relationship of the proofing entity with the individual, what information they have. And going at it from the level of principles, laying out the objectives is probably a good approach for policy. Maybe the Standards Committee can recommend some things, but if we're getting into really looking at evaluating and trying to objectively determine hard-core requirements, then it's probably time to call in NIST and others who do that type of thing.

Paul Egerman – Software Entrepreneur
Yes, that's correct.

Deven McGraw – Center for Democracy & Technology – Director
I think that's a great idea. I think we've started to articulate some of them on this call. One of the things that we can do is start to shape that into a set of straw man principles for either our next call, if we have time to focus on it, and if not a subsequent call, because some of this is more policy than technical. It's sounding like people are comfortable with that approach. We've already had a number of things come up, leaving some flexibility but making note of the need for example when you're establishing identity remotely, making sure that you're using mechanisms when you're talking about being able to actually access patient data in an EHR that is going to uniquely identify the individual. So how about if we do that?

Paul Egerman – Software Entrepreneur
Write up this discussion, is that what you're suggesting?

Deven McGraw – Center for Democracy & Technology – Director
Yes, in other words to try to do some work off line based on the discussion that we've had on a set of principles that we can talk about in a subsequent call. I'm not trying to prematurely cut off discussion, but it sounded like we were—

Paul Egerman – Software Entrepreneur
I think that makes sense.

Deven McGraw – Center for Democracy & Technology – Director
—... some consensus.

Paul Egerman – Software Entrepreneur
I think that makes a lot of sense. These were good comments about making sure that the online approach is not used for some ulterior purpose or ulterior motive. Also Neil's comment about the provisional, if that's the right word, you've got to allow people to—

Neil Calman – Institute for Family Health – President & Cofounder
I would just say making reasonably sure, as opposed to making sure.

Deven McGraw – Center for Democracy & Technology – Director
Right. ... reasonable person.

Judy Faulkner – Epic Systems – Founder
If I could add just a little bit of experience here, we have about eight million patients on the PHR and we haven't yet ever had a report of any misuse of the identity. But what we do see, and this is reporting what we heard from the VA, was that if the method is complex people just don't sign up. So I think that needs to be weighed in there.

M
Judy, are you talking about Lucy or MyChart here?

Judy Faulkner – Epic Systems – Founder
MyChart.

Paul Egerman – Software Entrepreneur
Great comment, Judy, because that's what we always have is these issues with any kind of security discussion is you've got to balance risk with utility.

Judy Faulkner – Epic Systems – Founder
What we found works the best is really when the physician or nurse after an office visit takes the patient right to a computer and says, why don't you log on? That works the very best. What we have found, strangely enough, is if they give the person a complicated log-on code they'll never use it again. Even that has to be simple. The whole process has to be simple.

Paul Egerman – Software Entrepreneur
Yes, that's a great comment, Judy, because when you do that the picture I have is you're actually accomplishing two purposes. One is you are in effect doing in person identity proofing, and the second thing, though, is you're actually promoting the use of the portal. Having them log on, that's like a training experience, they get to see it, and so that strikes me as really a best practice. That sounds really interesting.

What we're going to do is, I think Deven described it really well, we're going to try to do our best to write this up and create some sort of straw man working document on the policy. There's a second chapter to this discussion of user access, which is the authentication piece, so what you see on your screen is a slide that we've shown you before. It defines authentication. So that means after you've identity proofed the individual what is the process by which the person can use the system. What do they have to do?

So you see at the bottom are these four bullets or four circles. The first one is identity, second is identifier, so that's like a Social Security number, so this is authentication, which is the process of user name, password, keys, biometrics, whatever that authentication process is. So now, we're talking about authentication of patients, and there is this set of principles that have been put together that are very helpful for us. You want to have a method that is accessible to most of the population, thus, your consumers should have choices, although I actually have to say I have some questions about that. The consumer may want to have a choice but it's not clear that the software can do whatever the consumer wants.

The third thing is authentication services need to be transparent and employ oversight accountability, redress, there's the audit trail, there's the issue of any third party should be observable to consumers, the third party access, and authenticating entities should provide ongoing monitoring of access. So we have these principles and then we have this question that we need to answer. What is the acceptable method of authentication? What level of assurance is appropriate? Is single factor authentication acceptable? Should we make recommendations for additional authentication factors under some circumstances?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'm always the first one.

Deven McGraw – Center for Democracy & Technology – Director
Somebody has to go first.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think most of our experience now is shaped by the degree to which we use online banking, online stockbrokers, online shopping and so forth. Where on the one hand shopping may be overly simple because it's easy to quantify and limit the risk associated with it. It's only money and it's not that much money, we clearly have a problem where the risks for accessing healthcare data include all the risks of identity theft and go beyond that, and there's less of an obvious remedy in terms of giving money back. You can't put the information back in a tube of toothpaste.

Nonetheless, what I have learned about my banking and stockbroker places are that they use generally a graded level of risk assessment based on factors such as are you logging in from a device you have logged in from before. Is that device a device that's used for a lot of different peoples' log-ins, or is it one that has been solely yours. They tend to be variable in terms of when they say what was your mother's maiden name or whatever the question is, based on a real time risk assessment. So I think that—again, I may be channeling Dixie here—we need to talk about principles and the fact that this cat-and-mouse game between the good guys. The bad guys is going to go on and we need to be talking about this being variable based on some kind of assessment of risk or something like that, or assessment of threat.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
You were channeling me. I agree. It seems to me, Paul and Deven, that I think this whole conversation is around stage two. Even though we may say that we don't want to prescribe specific policies, I guess this is the question, do we still need to say for stage two that the organization ... has a process for identity proofing and has a portal that requires authentication, because the patient portal isn't really covered by HIPAA. Well, I guess it would be.

Deven McGraw – Center for Democracy & Technology – Director
Yes, it is.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
If it's tethered it would be covered by HIPAA.

Deven McGraw – Center for Democracy & Technology – Director
Yes, it is.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We don't even need to say anything. Do we need to say anything about the identity proofing at all?

Deven McGraw – Center for Democracy & Technology – Director
I don't know that we need to necessarily to make sure that the right technical functionalities get triggered. But I think one question is if we want to build in the capability in these portals to accept two factor, and I don't know if that makes any sense from a technical standpoint, if in fact either the institution wants to go in that direction or patients might ask for that additional level of security. I'm teeing that up. I don't necessarily have a formed opinion about that, but in thinking about whether we need to make sure that

the stage two EHRs, assuming that the portal recommendation goes all the way through the process, are able to accommodate policy choices that might be made by entities participating in meaningful use.

M
Here's an interesting question, do we want to set minimums, which I think the answer is probably uncontroversial yes, do we want to set upper bounds or do we want to let any institution that wants to exceed the minimum do so. The only argument in favor of setting upper bounds has something to do with people who use security as a way to prevent access rather than—

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
But when I think of the Betty Ford Clinic and other specialized situations, it seems clear that there probably is no widespread upper bounds that we could set.

Paul Egerman – Software Entrepreneur
This is Paul. I think that's right, although you look at a lot of necessarily comments about that specific clinic or if you look at an organization that does say "substance abuse" and possibly one that does say "reproductive health," my guess is that they might not even offer a patient portal. Or if they do they really would lock it down very carefully for lots of reasons. But the more fundamental issue, I think as you said, Wes, do we want to establish a minimum standard to correctly frame this discussion. The previous discussion we had about identity proofing is an area where we're going to have policy or principles. When you get to this authentication issue in stage two of meaningful use it is likely that there will be a requirement to use a portal, and again to frame the portal, it will probably be a situation where patients can view data, possibly they can download data, possibly they can print information, so that they probably can't change it. My guess is they may be able to have some other administrative capabilities, perhaps update like a phone number or an e-mail address or something, but they probably can't do anything about changing their own health record itself.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Paul, I wouldn't rule out them entering data about their health status.

Paul Egerman – Software Entrepreneur
Yes, but more likely that would be in the form of secure messaging to their—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I don't think so. I think that when you consider the kinds of things that you might want to track with cooperative patients at least, with engaged patients at least, what would be more convenient for them than logging into a portal and filling out a questionnaire.

Paul Egerman – Software Entrepreneur
But I'm thinking about what's actually going to be in stage two of meaningful use. I suspect that won't be there.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Okay. All right, I'll buy that.

Paul Egerman – Software Entrepreneur
But my comment is that I think we want to establish a minimum standard that will be in the certification criteria. In other words, I see minimum standard but I'm using the word "standard" incorrectly. Minimum—

Deven McGraw – Center for Democracy & Technology – Director
Policy.

Paul Egerman – Software Entrepreneur
Minimal policy concept that will be translated into certification criteria as part of stage two of meaningful use. So the question is, is single factor authentication acceptable for that minimum level?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I vote yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I would say yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well, if Dixie and John vote for it, I'm not going to go against it.

Paul Egerman – Software Entrepreneur
Yes, you almost become afraid, right?

Deven McGraw – Center for Democracy & Technology – Director
Let me just ask a question, because I'm inclined to vote yes too, but what would be the obstacle that an organization would face if they got a certified stage two EHR. Or their existing EHR was upgraded to include a portal that just had single factor authentication but they wanted to, just as a matter of policy, put additional factors in there or require that CAPSHA function to make sure people aren't screen scraping, the one that requires you to enter the word that you see on the screen. Is that something that's hard to retrofit in? I just want to make sure we're saying what we need to say on the technical side to accommodate some additional choices.

Paul Egerman – Software Entrepreneur
It's a good question, Deven. It really depends on the software and the software vendor, whether or not the software vendor will offer that flexibility. In other words, if we say single factor is the minimum acceptable, that's what all of the certified vendors will end up programming to. But if the physician buys the system and it does single factor and the physician wants to do something more, they've go to work that out with the vendor.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I don't quite agree with your assumption, Paul. It is the case that we can guarantee that the vendors will program to the minimum requirement, what's required by certification, but if they proceed to market for more there's nothing in our recommendation that would preclude them from offering more.

Paul Egerman – Software Entrepreneur
That's right. But I was trying to respond to Deven's comment, how hard is it. In some sense it's easy. They can go out to the marketplace and get whatever they want. But in another sense it really depends—usually once they've bought a system it's not easy for them to change.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Not in a small physician's office. If in fact, it's a remotely hosted product it's virtually impossible for them to change it.

Paul Egerman – Software Entrepreneur
Although on the other side, there are vendors now, I've become aware, who are looking at patient portals as their product and so the concept of modular certification, I suppose there would be marketplace solutions where you could do this, where that would be available.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, your original plan, I think, stands. It really depends on the vendor, but in general even systems integrating a third party product is a challenge for a small office. So it depends on the vendor. We're not saying anything that precludes any vendor offering more, but the fact is that whatever we set as the

minimum is likely to be more like the median or the third quartile anyway in terms of functionality available in products.

Josh Lemieux – Markle Foundation – Director Personal Health Technology
Back to authentication, this is after somebody's been proved, whether or not user name and password is a minimum standard, certainly what's in practice today for billions of transactions on the Web of sensitive information. Do we want to have some reference to a requirement for strong passwords, or password strength? Certainly when the Markle workgroup looked at this for a while and came out with recommendations, they did say user name and password, it's imperfect, but it's okay, but we do recommend enforcement of strong password. Of course that would have to be defined, but—

Joy Pritts – ONC – Chief Privacy Officer
Josh, unless there's been a change recently, it's my understanding that there's no industry accepted standard of what constitutes a strong password right now.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, and also Peter … testified at a hearing a year ago for one of our committees that there's very little incidence in the directory of incidents about people shoulder surfing to get passwords or things like that. There are some obvious ones. If your son's name happens to be a strong enough password then you've almost guaranteed that your hostile ex-wife can guess it.

Paul Egerman – Software Entrepreneur
Wes, you're always good for a great example.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Especially when it involves hostility and spousal relations. I think the notion of what is a strong password is slippery. We want to have some policy that encourages people to use strong passwords, but I can remember under HIPAA having to help people deal with their accounts ... insisting that passwords had to be 12 random characters to pass HIPAA. We've already learned through the experience through the VA that making this overly difficult, particularly where we don't have a real proven benefit, inhibits use.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Might I add that good password hygiene is something we all like to think that people use. To Wes' point, though, the more difficult you make it for people, often the less likely they're going to want to engage and use the service. I think that transparency and the like, I think what we can try to do or what we can make recommendations about, and there are tools available in the market that allow people to see how strong their password is as they're creating it. It doesn't mean that they have to choose a strong password or weak password or whatever, but there are tools out there that will actually help tell the user whether what they're typing in is any good or not.

Carl Dvorak – Epic Systems – EVP
One of the things I want to just remind people is that the real protection behind the password is how many attempts you let a person try before canceling their account, requiring them to reestablish their account. That generally is the real protection behind the password and it usually makes up for the non-immediate guessable passwords. So if you—

M
Or the programmatic attempts where they try to just keep going through it and hitting different password combinations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what we got out of the, this is Dixie, the hearings that Wes referred to. I'd like to go back to this question that was brought up about how easy it would be to upgrade to two factor and relate to you something that I learned just this week that is sort of disturbing in this respect. This had to do with an organization who bought a certified EHR and they wanted to use a different audit reduction tool than the one that came with the EHR. The vendor warned them that if they used something different in there it

would negate the certification itself and they couldn't get their reimbursement because it wouldn't be using a certified EHR. So I think that it seems to me we need to make it possible for somebody to take a certified product and upgrade it two factor and not lose their certifications.

Paul Egerman – Software Entrepreneur
Yes, and that's a good issue, Dixie. I'm familiar with that issue, but it's a separate issue.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But it really isn't, I don't think, because what I'm going to suggest is maybe that we suggest, well—

Paul Egerman – Software Entrepreneur
All I can tell you is it is possible to do.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
It is possible to do. The reason the vendor said that is also an interesting and complicated issue.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Do you think we need to have downstream a certification criteria that says that it's possible to upgrade to two factor, or can we just ignore it?

Deven McGraw – Center for Democracy & Technology – Director
I think as a specific authentication standard is not specified for certification, then just the requirement of single factor in the system shouldn't lead to the problem that you just discussed.

Paul Egerman – Software Entrepreneur
That's correct.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I want to make two points here. One is that unless that other issue, that other issue has come up all over certification, it's sort of a fundamental issue about certification, and it needs to be addressed. If it's not addressed it's not that clear we can do that much on our side to fix it. But the other thing is, we said earlier that user name and password is being used for billions and billions of transactions or however Carl Sagan counts stars, and I'm not sure that that's true. The concept that we see more and more in the financial services industry is what they call multi-factor authentication, where multiple implies more than one but not necessarily two.

Paul Egerman – Software Entrepreneur
Let's back up. I had asked the question is single factor authentication acceptable, and I thought everyone said yes, but you're saying now no, you want to do more?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
You're right. I'm sort of backing up here. At a minimum, I want to enable that, not—

Paul Egerman – Software Entrepreneur
Well, what we clearly want to do is we want to be clear that single factor is the minimum and that there needs to be capabilities to do more.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And not get into the password, how many letters and how many—

Paul Egerman – Software Entrepreneur
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
—... all that.

Paul Egerman – Software Entrepreneur
Let's do our best to go through this one-step at a time. We want to say single factor is the minimum. I think we've got agreement that we don't want to do a requirement for 35 characters in the password. We don't want to do that.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Thirty-four will be fine.

Paul Egerman – Software Entrepreneur
Right. And so the other thing that I just want to make sure that we close out, there was a comment from Carl about password attempts. I think in the industry it's frequently called "three strikes and you're out." Do we want to say anything about that topic?

Leslie Francis – NCVHS – Co-Chair
Can I jump in on that one?

Paul Egerman – Software Entrepreneur
Yes.

Leslie Francis – NCVHS – Co-Chair
If people need emergency access, I can see nervous people making mistakes. In some ways I think knocking the three strikes and you're out is riskier, so somehow there has to be a balance of risk factors whether it's—

M
Portable devices now typically is ten strikes and you're out.

Carl Dvorak – Epic Systems – EVP
Yes, I don't suggest three. I think that's too little. What you're really trying to protect is the computer program running 10,000 iterations to try to—

Leslie Francis – NCVHS – Co-Chair
Exactly.

Carl Dvorak – Epic Systems – EVP
Ten, fifteen, anywhere in that neighborhood is clearly—

Paul Egerman – Software Entrepreneur
My question is do we want to set a minimum standard on that issue, or do we want to make that a best practice?

M
I think we should make it a best practice that describes the process rather than the number of attempts.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'd like to suggest that the system ought to be certified to have the capability to do that, that the number of attempts not be part of the certification.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I agree.

M

What you're trying to do is prevent the programmatic attack, as Carl stated, and frankly you can give them 100 attempts and it still would probably prevent programmatic attacks because they will go and hit thousands upon thousands of combinations.

M
Yes, but just thinking about the certification process, it's pretty easy to say a minimum requirement for a certificate is that there's a site specified number of attempts without a successful log-in after which personal contact is required to log-in.

M
I agree.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I agree.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
By the way, we shouldn't say that, though, either. My apologies, but we've also found that to prevent programmatic attacks if you simply lock out the account for an hour or two hours we'll also frustrate that attack, too. So you simply have a time out period, is often very effective.

Paul Egerman – Software Entrepreneur
... also have a situation where if you fail two or three times you would start to get a successively longer lock out. So at the end of three times you would be locked out for 15 minutes. Then you—

Carl Dvorak – Epic Systems – EVP
Paul, there really are three levels to think about. One is the programmatic attack, and you're right 150 would eliminate that. But second, though, is a closely related person who might have some history of your other passwords, there if you had 150 times to try to guess my wife's password, chances are good I might get it. So I think some number that takes both of those factors into consideration would be good, and yet not so few that I'm going to mess it up myself.

Paul Egerman – Software Entrepreneur
My question is, what are we saying in our recommendation? Is it left open? Do we let the Standards Committee deal with what they want to do for prevention of programmatic attempts? Do we want to set a number ourselves?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Carl said two of the three I think that he wants to say, but I think we should agree that we're interested both in programmatic attempts and repeated attempts by someone with close knowledge. It gets back to what Leslie was talking about. I think we should create a requirement that all systems be certified to have some capability. I don't know that we want to, unless we're talking about some sort of meaningful use audit or something like that in terms of how the system is actually used in production. I don't think we need to get into the specifics of the number or whether it's a progressively longer space or whether it gets longer on the 217th try or what, but we ought to get the minimum capability into the systems.

Deven McGraw – Center for Democracy & Technology – Director
If you think about the way that some of the certification criteria in the security space is worded, they're worded as capabilities without reference to specific standards or particular methodologies. But there's, for some of them, some description about what needs to be part of that and so in this case it would be some capability to cease access.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
To inhibit further access—

Deven McGraw – Center for Democracy & Technology – Director

To inhibit access addressing both programmatic attacks as well as repeated attempts by someone with close knowledge. I wrote that out because I liked the way you framed that.

Paul Egerman – Software Entrepreneur
So it sounds like that's a conclusion or an answer to this question. Do we need to say anything more? Do we want to be clear this is a minimum and for some high-risk situations you might do more?

M
We want to be clear that there's nothing in this that inhibits stricter administration of one factor authentication. We're simply setting a minimum.

Deven McGraw – Center for Democracy & Technology – Director
You can set more for legitimate security reasons, not to provide a barrier to people actually using this tool.

Paul Egerman – Software Entrepreneur
That's great.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We've been really careful not to change HIPAA in all of our other discussions. Do we really want to recommend something that is stronger than what's in HIPAA?

Deven McGraw – Center for Democracy & Technology – Director
Well, what we're doing, Dixie, is we're triggering system capability.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I know but—

Deven McGraw – Center for Democracy & Technology – Director
But not necessarily requiring people to turn it on.

Leslie Francis – NCVHS – Co-Chair
HIPAA requires a risk analysis, and all we're saying is that this needs to be a capability that if people choose to do this, it's there.

Paul Egerman – Software Entrepreneur
Yes. Or another way to look at it, Dixie, is we're defining a minimum level that will be in the certified EHR for this function.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
For this function, okay.

Paul Egerman – Software Entrepreneur
I think it's a good thing to do, and I think we've made great progress.

Deven McGraw – Center for Democracy & Technology – Director
Can I just ask one question, because I realize that the slides didn't squarely tee this up? I assume we want audit trail functionality for the portal.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Egerman – Software Entrepreneur
Yes, I thought that wasn't part of this discussion, though.

Deven McGraw – Center for Democracy & Technology – Director
Okay, fair enough.

Paul Egerman – Software Entrepreneur
I was told to accomplish one issue and I think we did it. I think we're ready to move on to the next topic.

W
Okay.

Deven McGraw – Center for Democracy & Technology – Director
Terrific.

Paul Egerman – Software Entrepreneur
It's a good discussion.

Deven McGraw – Center for Democracy & Technology – Director
Yes. All right, so as I indicated in my ... we will take on some other policy issues that are related to patient access to information in a provider EHR such as some of the transparency issues that the VA raised briefly in their presentation. I know for those of you who are familiar with the Blue Button Initiative, there's a set of policies that Markle put together, through its customary consensus process, that are worth thinking about. But since they're not tied to the need for certification criteria, we're going to come back to those. I just wanted to make sure people were aware that I think we have some transparency issues that we should discuss, but we don't have to do those now. We will reserve some time to get to those so that we can spend more time talking about things that do have technical components.

So with respect to stage two of meaningful use, we are both in the early stages of talking about this and yet still facing some pretty significant deadlines. In part, because the Policy Committee and the Standards Committee have processes that they need to go through and all of that work has to really be finished in sufficient time for the agencies to do their rule making, which they need some time to do in order to be able to issue the stage two meaningful use rule. I think at the end of the calendar year is the target, if not, beginning of next year. But that's the reason why, as I said in the beginning we are trying to think about what's been put on the table for stage two of meaningful use in the other functional categories, like treatment and care coordination, public health reporting, information exchange. Also taking a look at our other recommendations and trying to identify those that we might need to tee up more clearly for the Policy Committee so that they can be potentially turned into certification criteria where that's necessary.

What we did here was try to create a potential short list, again, based on meaningful use objectives that are either from stage one or that have been proposed by the Meaningful Use Workgroup for stage two. So that process isn't final but we're trying to be forward thinking and anticipate what might happen as part of this whole process and then think about which of those policies link to certification requirements so that that can be, again, presented to the Policy Committee ideally in April. That's certainly our goal.

We just talked about the patient portal issue, which is the first one here on the chart, and went through some principles for identity proofing. Again, those don't have a technical component, so we have a little bit of time to work on those principles. But we came up with some consensus on authentication which we will wordsmith and be able to discuss at our next call, and then I think we just decided that we wanted an audit trail, but we can come back to that because we spent about two seconds on it.

The other issue that we teed up here is authentication of an entity, and this is related to the meaningful use objective of information exchange, which is still being scoped out but currently is described as connecting to three external providers or establishing a bidirectional connection with an HIE. We have already said that entities should have digital certificates, and in fact, I know that the Privacy and Security Workgroup has begun doing some additional work on that. With respect to user authentication, which is relevant to ePrescribing, we said performing a test of HIE, that's really a stage one meaningful use requirement, but generally we have been talking about this user authentication issue. Noting that at least for the ePrescribing of controlled substances that the DEA already requires the ability to have two factor authentication with some specific requirements around that.

Then we also have been working on some recommendations of our own that apply to user authentication, both within and also for remote systems, and we will set that aside for now because we're still trying to finalize that language. But what I'm presenting here is just what we thought was a landscape of things that we might want to tee up because at least as an initial matter we want to make sure we have the universe of what we want to consider and then we can start drilling down on some of this stuff.

Then there is the privacy and security category, which presently requires the performance of a security risk assessment, and whether we want to say something specific about needing to do that also for stage two, and we have some additional slides on this, whether we want to say something more specific about addressing the functionalities that are in EHRs. We can talk a little bit about what the HIPAA security rule already requires, because certainly all of the entities that are participating in the meaningful use program are covered by HIPAA already, and if they're not then they will be when they're doing electronic transactions. I think I'm right about that. Adam will correct me if I'm wrong.

The last category put on the table was some of the recommendations that we came up with in the patient matching context and whether there's some certification work that needs to be done with respect to the demographic data fields and the specific recommendations that the Policy Committee already endorsed in that category. So let me start by saying, again, is this a good universe of policy recommendations that are tied to technical functionalities that deal with the meaningful use transactions that are already proposed on the table, and issues that we have already as a tiger team discussed. For the most part teed up to the Policy Committee for endorsement, we're working on a few, but in terms of what we have pretty significantly in the pipeline versus something that's brand new.

Is there anything that anybody thinks we've left out, is the relevant question? If it wasn't clear from that blur of words.

M
So you're not asking us to comment on a specific item here, but just to mention anything that's missing?

Deven McGraw – Center for Democracy & Technology – Director
Yes, and then we'll get to specific items. Okay, now you can go to the specific items. Let me just ask as a threshold matter, since again we spent about two minutes on the audit trail issue for patient portal, was there anybody who disagreed with the need for an audit trail capability for a portal if one in fact is required as part of meaningful use?

M
What's the audit trail supposed to do in the client ... in terms of a portal?

Deven McGraw – Center for Democracy & Technology – Director
I think it would look a lot like what the audit trail functionality is for EHRs generally today, which is recording actions. Actually there's a specific standard, which is date/time identification of the person accessing it, and then the ability to generate that log, which I think ideally the patient could review.

Leslie Francis – NCVHS – Co-Chair
It would let you know if your wife is logged in.

M
Basically, this would only be of practical value if you were ... accessing to somebody else.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
No, there's two values. One is effectively someone says there's some situation where someone says I tried to look this up and it wasn't there and my health was compromised. If you have a log you can show if they were there or not. The other situation is there is a question about how some information got out, and previously under the audit for EHR users they would ... have a complete list of who at least logged

into this case. That would be incomplete without also having an audit of portal log-ins, so that's important.

Then finally, an issue we can consider is for the case where someone is concerned that another person may be accessing their data. Do we want to have a requirement that says that viewing the history of transactions for a given user, the audit trail for a given user in a user-friendly way, should be a requirement of the portal? In other words, it's one thing to go to the security officer and get that person to dump a security log and tell you what happened. It's another thing to be able to do it on a self-service basis.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Just to provide some HIPAA background on this, HIPAA does require that a covered entity maintain audit logs and that would include the patient portal, which is not to say one way or the other as to whether that should also be included in certification criteria for EHRs or meaningful use criteria. There's no requirement under the security rule or the privacy rule to provide the patient with access to that auto log, which goes towards what I believe Wes was just saying.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I would further say that nobody except in extreme sys admin type is the least bit interested in reading an audit log. Accounting for disclosures is supposed to be human readable, but audit logs are never human readable.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That's why I said a user friendly function. When you have a specific issue like who logged in under my user ID portal, it's not that hard to send out a user friendly version of that log. In general, you can't allow end users to access audit logs because there's information about every patient in there. But this is the specialized situation. I'm not as keen on that point as I was on making it a certified requirement that the audit log include log-ins for the patient portal.

Paul Egerman – Software Entrepreneur
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Neil Calman – Institute for Family Health – President & Cofounder
Since it's a portal into the EHR, how would you design an audit trail for the EHR that wouldn't include remote log-ins? It seems like it would be part of the regular audit trail of the EHR access.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that's it.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
It would be pretty easy to buy a third party's portal package and have some difficulty with that interface and say oh, it's not required. We won't do the audit trail part. I think it's worth making it a tested part of certification.

Josh Lemieux – Markle Foundation – Director Personal Health Technology
I agree. It should be able to log not just accesses but, for example, downloads, if somebody downloaded something. Somebody logs in, they download, that should be tracked and able to be counted.

M
This gets into an enormous amount of detail here that I think we have to be incredibly careful about in terms of ....

M

I'm wondering, Josh, why you want to single that out, given that it adds a lot of complexity to testing and everything? Fundamentally, I can do a print screen with anything that's on the screen anyway, so whether I downloaded it or whether I captured it by some other means is the second order in terms of importance, it seems to me.

Josh Lemieux – Markle Foundation – Director Personal Health Technology
Yes, I can understand that. It may help the provider be able to show the ability to respond to requests for electronic copies in an automated fashion. So it would certainly be something that I, as a doctor, would want my system to be able to do, to be able to count those kinds of things.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, I think anything that the physician might be required to do under meaningful use, there should be a certified function of the system to do it. So if the physician is required to report how many patients downloaded their data, then we would want there to be a certification criteria that says you can count how many patients downloaded their data.

Josh Lemieux – Markle Foundation – Director Personal Health Technology
Yes, that's what I'm getting at. I know it's a little bit outside of privacy and security, which you're talking about now, but certainly if delivering electronic copies is one of the things that is already a requirement, the certification requirement for qualified health IT should make the ability to count that automated so that it's easy for—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Josh, I'm very sensitive to the fact that Markle Foundation has criticized previous criteria for being overelaborate and I would not want to put anything more into the minimum requirements than what is a true minimum that even a disruptor innovator we would expect them to do it.

Paul Egerman – Software Entrepreneur
I don't mean to interrupt. But, Deven, I just want to do an agenda check. Is this where we want to be right now, in terms of—

Deven McGraw – Center for Democracy & Technology – Director
I think we want to try to start to close this part of the conversation just for this call, because we have two more calls now scheduled, Policy Committee. But one thing I just want to add is the portal and what kinds of functionalities need to be part of it is still a little bit of a moving target in terms of whether it will be part of meaningful use. Paul, I know that the PCAST Workgroup has been looking at portals that would include a download function and so in that respect that does change a little bit about what you might want to track in an audit trail. But I think for now I'm hearing that functionality of an audit trail for the portal we should leave on the list as we continue to iterate this. Also, keep in mind the role that the Standards Workgroup play in fleshing out the certified patient criteria in more detail, since our role is really to talk policy and let them fill in the required functionalities and standards, right, Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's right.

Deven McGraw – Center for Democracy & Technology – Director
Okay. So because we had a super packed agenda, actually I felt we did really well on this call, I have to say. I want to try to tee up where we're going to be doing some follow up work. That is to take this matrix of potential policy issues to tee up for meaningful use stage two with a focus on those that translate into required certification criteria and talk more about these categories, since it sounds like nobody thought we left something out. But there certainly is an opportunity to weigh in on the interim if in fact you think we have left something out given your thoughts.

Then of course we've got some recommendations that came up on our call today that we need to develop language, straw dog, as Micky Tripathi likes to put it, straw man for you traditionalists out there, for you to weigh in on, which brings me to where I'm going to skip to because this is homework for the workgroup.

That is we have been spending a lot of time talking about user authentication and we actually had a much easier discussion on patient authentication than we did for EHR user authentication and maybe that discussion will help us to refine these recommendations a bit more, given the clarity that we were able to reach in that context.

But nevertheless, what Paul and I and team MITRE, with assistance from Joy, did was to try to work up what we thought was the consensus that we reached. It was probably a pretty rough consensus, but the consensus that we reached by our last call on user authentication, and then I'll ask you to read these off line and provide some feedback. But essentially it captures the idea that we ideally wanted two factors, but were not totally comfortable with the NIST or DEA articulation in terms of what those factors would be required to be, but acknowledging that certain sensitive transactions might require some more specificity and noting that additional work on a use case basis might be needed going forward.

The other thing that this notes is that while we initially engaged in these conversations focusing on remote access, at least on our last call, because we were having difficulty defining what would be considered a remote access versus an internal access. We tentatively landed on the idea that we wouldn't make that distinction in terms of the baseline authentication recommendations that we would be making. I've had some offline conversations with a couple of folks who are still thinking that a requirement beyond a user name and password for access within the physical confines of a facility or a physician practice feels a little burdensome, I think we can continue to try to talk about that and hone that. But I just wanted to tee up for you that at least on our last call we thought that we couldn't make enough of a distinction between what was really remote and what was internal to make a difference from a policy standpoint.

Then we have some other recommendations about needing to continually reassess these policies, which by the way the vehicle for advancing them, at least from a policy context, is NW-HIN governance, but of course it does have certification implications if two factors or more than one factor is required. We also have some language about ONC doing some work to develop and disseminate evidence about the efficacy of various methods for authentication and continually reassessing NW-HIN's policies. Also making sure, I'm not sure I mentioned this, that they're consistent with national identity efforts such as the National Strategy for Trusted Identities in Cyberspace, for those of you who are familiar with that effort.

So therefore, if you think about a requirement that user authentication be at least two factors, and acknowledging that the DEA rule is in effect providers who prescribe controlled substances will need to comply with it. But it seems as though from a certification standpoint there might need to be the capability to at least be able to honor the DEA rule in terms of authentication.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I have a question, Deven. In these items when you refer to the Nationwide Health Information Network, are you talking about the NHIN Exchange only or Direct as well?

Deven McGraw – Center for Democracy & Technology – Director
No. What we're talking about is the governance process that we still don't have the details on, that will be the voluntary effort, voluntary governance that are the standards and protocols for exchange that the Policy Committee. We had an entire workgroup developing the process for this, there's a rule making that's going to come out in the fall that's going to establish the conditions of trust and interoperability that people are going to ascribe to. It's my understanding, although I think we're still waiting on the details of this, is that the participants and those current NHIN Exchange efforts are going to be asked to be part of the NW-HIN governance effort as it's developed. Joy, please correct me if I'm wrong about that.

Joy Pritts – ONC – Chief Privacy Officer
I don't know.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Joy Pritts – ONC – Chief Privacy Officer

We're at a place where it's pretty hard to tell exactly what the scope is or how that might be achieved. There have been a few different models that were proposed in discussions through some of these workgroups. One model was I think the NW-HIN, it would be focused on the, I hate using all these acronyms but the HIST level, but that it might flow down to the actual participant end user level. I think somebody else had suggested that all participants be officially part of it. But you can read some of the recommendations where you would see that there are pluses and minuses of both of those approaches.

Deven McGraw – Center for Democracy & Technology – Director
Yes, I think, though, that the focus on NHIN or NW-HIN governance was that we went to that place to see, based on the specific recommendations of David Blumenthal at the last Policy Committee meeting, that he invited us to establish a higher bar than HIPAA might require, for example, for authentication for NW-HIN participants. So we went for it, at least in the draft recommendation.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I was on vacation for a week here, but is every user of every EHR and perhaps every patient who logs into a portal of an EHR a user of the NW-HIN?

Deven McGraw – Center for Democracy & Technology – Director
No, I don't think so.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
My beady little eyes zeroed right in on that when you put up the chart, was how did we get from discussing access to an EHR to NW-HIN governance? That seemed like a big leap to me.

Deven McGraw – Center for Democracy & Technology – Director
Here's how we got there, Wes, which is to say that we got there in terms of what are the policy levers that ONC has available in order to advance some of the policy recommendations that we have made that go above and beyond the baseline that HIPAA would require, because we don't advise OCR. We're lucky to have them on our calls. It's very fortunate for us, and particularly to remind us of all the things that HIPAA already does that we don't necessarily have to repeat. But to the extent that we've gone above and beyond the meaningful use criteria as a vehicle for enforcing a higher set of expectations, is a vehicle that CMS at least expressed in stage one that it wasn't interested in doing. It was not interested in requiring additional privacy and security requirements beyond what HIPAA would require. So in talking about this at the Policy Committee, what's the policy vehicle, David Blumenthal specifically suggested that NW-HIN conditions of trust and interoperability, which is to form the governance of the Nationwide Health Information Network, is a policy vehicle that ONC is eager to use to establish that higher bar.

Joy Pritts – ONC – Chief Privacy Officer
And I think, Deven, that it's important to continue to focus on the exchange element there.

Deven McGraw – Center for Democracy & Technology – Director
Yes. So in other words—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That's the issue is ... exchange with the other. I can understand how it got there. I'm sure everyone will interpret this as humor when I say that's what happens when you take suggestions from a short timer.

Joy Pritts – ONC – Chief Privacy Officer
Wes, I don't know that David intended to reach down that way.

Paul Egerman – Software Entrepreneur
That's correct. I was there. I took David's comment as saying NW-HIN causes us to raise the bar on user authentication. Then I have to say I was the one who was encouraging, well, let's put it then in NW-HIN governance.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Paul Egerman – Software Entrepreneur
That's what's causing us to raise the bar. Let's put the—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
My concern is that the Governance Group has to somehow represent those that are governance and we've just increased that list to 600,000 users.

Deven McGraw – Center for Democracy & Technology – Director
Again, these are user authentication recommendations within a provider entity, not patients.

Joy Pritts – ONC – Chief Privacy Officer
Well, even if the—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
But that 600,000 is the users, right?

Joy Pritts – ONC – Chief Privacy Officer
Yes, that's what I was going to say.

Paul Egerman – Software Entrepreneur
A lot more than that, actually.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes.

Paul Egerman – Software Entrepreneur
You've got a couple of million people.

Deven McGraw – Center for Democracy & Technology – Director
Okay. But I think that that gets to the issue of what is the scope of the higher bar that we want to achieve. Again, the NW-HIN is supposed to be about policies for information exchange, and the higher bar that creates trust in information exchange.

Paul Egerman – Software Entrepreneur
Well, let's just—

Deven McGraw – Center for Democracy & Technology – Director
... point of that, of an information exchange is the log-on of an individual user at a system.

Paul Egerman – Software Entrepreneur
Let's do this, Deven, the way I'm interpreting this discussion, maybe I've got it wrong, is the topic is where does user authentication belong? Is it certification, or does it belong under NW-HIN? Or does it belong under both? Is that what we're discussing?

Deven McGraw – Center for Democracy & Technology – Director
Yes, what we're discussing, these recommendations have been developed for some time, so I think, number one, we are trying to finalize the substance of what we want to say on authentication. Then I think separately what's embedded in here is what's the policy vehicle for propagating that. Is it NW-HIN, and/or is it certification, or is it both?

Paul Egerman – Software Entrepreneur
Right, that's what I was saying.

Deven McGraw – Center for Democracy & Technology – Director

Yes. So it's both a substance and a process point. The main reason to bring this up at the 11th hour was not to try to get you to make a rash decision, but to put this back on the table and get folks thinking about it, sending us feedback so that we can hopefully iterate on it off line. I know everyone is really busy, but we basically have two calls left. We scheduled another call, so we have one and a half hours on another call and then two hours on another to try to get done at least what we want to do for meaningful use and certification. So with that focus in mind, we might have to put some stuff that's related to, say, NW-HIN governance to the side. But nevertheless, we should at least be able to get done what we need to get done and we're going to just have to continue to both work off line and try to be as efficient as we can on our call.

Notwithstanding that the universe is big of the things that we need to do, I actually thought that we got a lot done today. We will get out materials to you for you to iterate on between now and our next call. I think we should probably open the lines up for the public.

Judy Sparrow – Office of the National Coordinator – Executive Director
Operator, can you check and see if anybody wishes to make a comment.

Operator
I don't have any questions at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you, operator. Thank you, Deven and Paul.

Deven McGraw – Center for Democracy & Technology – Director
Thanks, everybody.

Paul Egerman – Software Entrepreneur
Thank you, Judy.

Joy Pritts – ONC – Chief Privacy Officer
Thanks. That was a really good meeting, everybody.

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes, it was.

Joy Pritts – ONC – Chief Privacy Officer
It was very efficient.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Deven is fantastic and so is Paul.

Joy Pritts – ONC – Chief Privacy Officer
Yes, and so are you all. That was just a very focused conversation. It was really very useful.

Deven McGraw – Center for Democracy & Technology – Director
Yes, thanks.

Joy Pritts – ONC – Chief Privacy Officer
Not that they aren't all. All of them are. Thanks a lot. Bye-bye.

Deven McGraw – Center for Democracy & Technology – Director
Thanks, everybody.

Public Comment Received During the Meeting

1. Relying only on passwords for access to PHRs seems weak. Maybe you should allow passwords only for access to the least sensitive info, but require 2 factors with a cell phone for more sensitive info

2. NIST SP 800-63 defines requirements for identity proofing at the different assurance levels.